VA Enterprise Design Patterns:

1. Privacy and Security

1.1. User Identity Authentication

Office of Technology Strategies (TS)
Architecture, Strategy, and Design (ASD)
Office of Information and Technology (OI&T)

Version 2.0

Date Issued: March 2016

THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION

Rodney Emery

Digitally signed by Rodney J. Emery 106229
DN: dc=gov, dc=va, o=internal, ou=people,
0.9.2342.19200300.100.1.1=rodney.emery@va.
gov, cn=Rodney J. Emery 106229
Reason: I have reviewed this document.
Date: 2016.03.24 19:35:39 -04'00'

____

Rodney Emery
Director, Technology Strategies and GEAC, ASD
ASD Technology Strategies

PAUL A.
TIBBITS 116858

Digitally signed by PAUL A. TIBBITS 116858
DN: dc=gov, dc=va, o=internal, ou=people,
0.9.2342.19200300.100.1.1=paul.tibbits@va.go
v, cn=PAUL A. TIBBITS 116858
Reason: I am approving this document.
Date: 2016.03.31 16:08:00 -04'00'

____

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

REVISION HISTORY

Version	Date	Organization	Notes
1.5	February 2016	ASD TS	Initial Draft/Outline of the update to the Internal and External User Identity Authentication Design Patterns issued for stakeholder review. Combined Internal and External Authentication Design Plan documents and updated the name. Changed format to provide future state relevant to all authentication, internal and then external. Added IAM Infrastructure Integrity Risk Assessment and Recommended Actions.
1.7	March 2016	ASD TS	Includes the additional updates: Added overview diagram. Updated As-Is state for SSOe and use of MVI. Updated Internal and External current state diagrams. Clarified goal of IAM to provide a single source to access all identities and attributes in use across VA. Added requirement to create LOA Assessment Examples specific to VA for every level and provided draft example. Updated Direct Client Authentication using PKI over TLS to be a temporary solution until SSOi supports LOA 4. Updated Use Cases. Updated scope to specify exclusion of Compliance Audit and Reporting (CAR), VA Credential Service Provider (CSP), electronic signature (eSig) and identity proofing (IP).

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
2.0	3/10/2016	Joseph Brooks	Privacy and Security Design Pattern Lead

TABLE OF CONTENTS

FIGURES

TABLES

1 INTRODUCTION

The Department of Veterans Affairs (VA) has a unified enterprise Identity and Access Management (IAM) program to coordinate the secure access to VA resources for both internal and external users. Office of Management and Budget (OMB) M 11-11 mandates that agencies "require the use of PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems" for internal users and contractors. External users such as other Government agencies, private sector parties, and citizens, including veterans, require varying levels of access to interact with VA services. This Enterprise Design Pattern is intended to outline enterprise guidelines for authenticating users via a standardized enterprise approach and authentication service that complies with established VA security policies (VA 6500 Information Security Handbook), Federal Information Processing Standard (FIPS) 200, and National Institute of Standards and Technology (NIST) guidelines (800-63 and 800-53 per Appendix D). The authentication services are also designed to be supportive of VA's current and future enterprise authorization and auditing guidelines.

1.1 BUSINESS NEED

Information system owners perform proper authentication by:

- Using approved identity authentication procedures that consider the importance and sensitivity of the information in a system.
- Recognizing the threats and vulnerabilities to the system.
- Considering the level of confidence in any user's asserted identity.
- Understanding the risks that are posed to the enterprise by the potential loss or exposure of information contained in the system.

Assessment of the system and the information it processes is directly tied to the level of assurance (LOA) (per NIST SP 800-63) and authentication method required.

VA has implemented Enterprise Shared Services (ESS) for user authentication through the Identity and Access Management (IAM) program. Use of these services constrains project-specific solution designs to a standard set of enterprise security services, which improves manageability and reduces the attack surface. These services will help VA address cybersecurity goals and objectives for protecting federated identity credentials and support the shift to two-factor authentication (2FA) where possible, as described in the VA Enterprise Cybersecurity Strategy (Version 1.0 released in September 2015).

1.2 APPROACH

To support the move to enterprise authentication services, VA is adopting NIST SP 800-63 LOAs and aligning appropriate authentication protocols to the level of risk posed by those applications. Standardization of these authentication protocols and technologies used by these applications will simplify application design, increase network security, and allow for proper user management. Projects will coordinate with the IAM Business Program Management Office (BPMO) to integrate their system with IAM services based on the LOA determination.

2 CURRENT CAPABILITIES AND LIMITATIONS

VA’s IAM program currently offers a comprehensive suite of services related to authentication. IAM provides the following activities through the VA Access Services (AcS):

- **Identity Proofing (IP)** – Verifies the identity and information used to establish a digital identity.
- **Provisioning (Prov)** – Process of associating a digital identity with one or more resource accounts.
- **Credential Service Provider (CSP)** – Provides credentials for users not eligible for other credentials being used by VA applications.
- **Single Sign on Internal (SSOi)** – Provides Single Sign On (SSO) for internal VA users.
- **Single Sign on External (SSOe)** – Provides SSO for users external to VA.

Initially, the user establishes a digital identity. This consists of providing information to the Identity Provider who will create the digital identity. The methods used to validate the information provided are rated based on the LOAs which are described later in this document. Once a digital identity is established, it is associated with one or more accounts through Provisioning. In some cases, this may occur at the same time as the last step. IAM may also serve as the CSP to create the account. External users whose identity is established by a VA-approved CSP can authenticate using the SSOe service.

Application owners can integrate with the SSOi or SSOe service as long as they can support Security Assertion Markup Language (SAML). The application will first go through a risk assessment to determine the proper LOA. This determines the authentication requirements. Attribute requirements should also be documented and provided. IAM’s Virtual Directory Server (VDS) can obtain attributes from multiple sources in support of authentication and authorization.

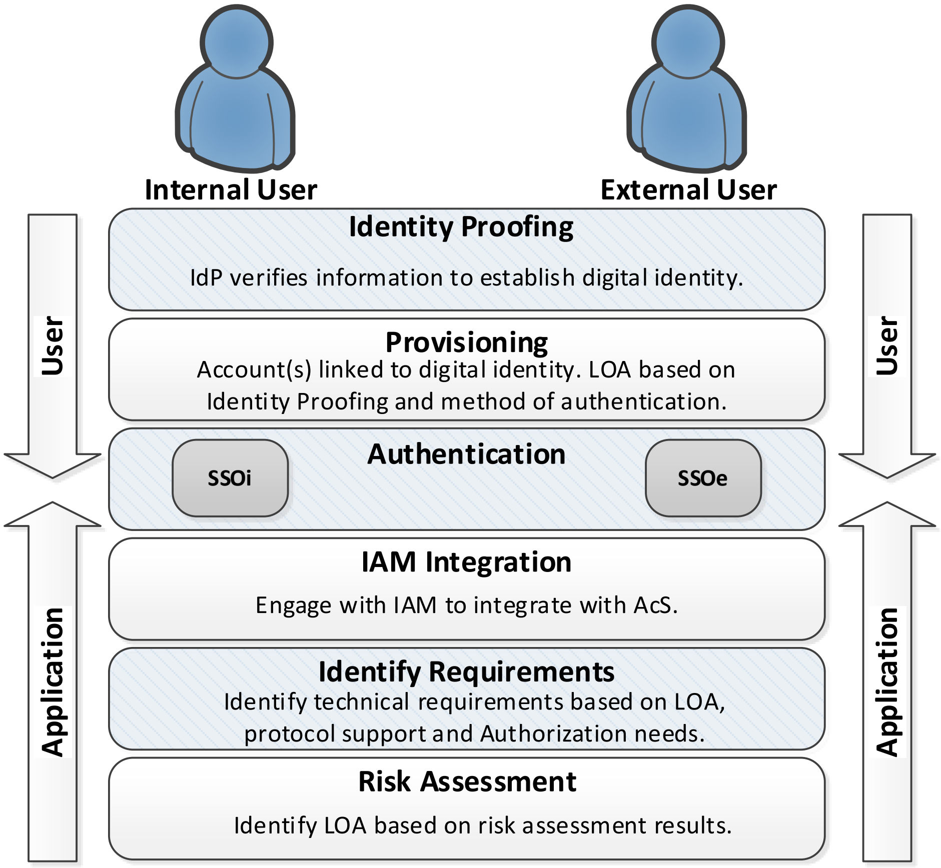
Internal User
External User
User
User
Identity Proofing
IdP verifies information to establish digital identity.
Provisioning
Account(s) linked to digital identity. LOA based on Identity Proofing and method of authentication.
Authentication
SSOi
SSOe
IAM Integration
Engage with IAM to integrate with AcS.
Identify Requirements
Identify technical requirements based on LOA, protocol support and Authorization needs.
Risk Assessment
Identify LOA based on risk assessment results.
Application
Application

Figure 1 – Overview of IAM Progression

2.1 INTERNAL AUTHENTICATION CAPABILITIES AND LIMITATIONS

VA currently allows the use of non-standardized processes to conduct internal user authentication to the network and to applications. VA policy requires Public Key Infrastructure (PKI)-enabled Personal Identity Verification (PIV) cards to enable internal user authentication to Active Directory (AD). However, some security projects do not integrate tokens with IAM and allows internal user authentication via the user's AD username and password, particularly for new users during the time when PIV cards have not yet been issued or when PIV card errors occur. Additionally, internal user authentication to the application layer is allowed via various non-standardized protocols. While all applications are currently required to comply with standardized security requirements established in VA 6500 and NIST SP 800-53, to date, VA has not standardized accepted authentication protocols.

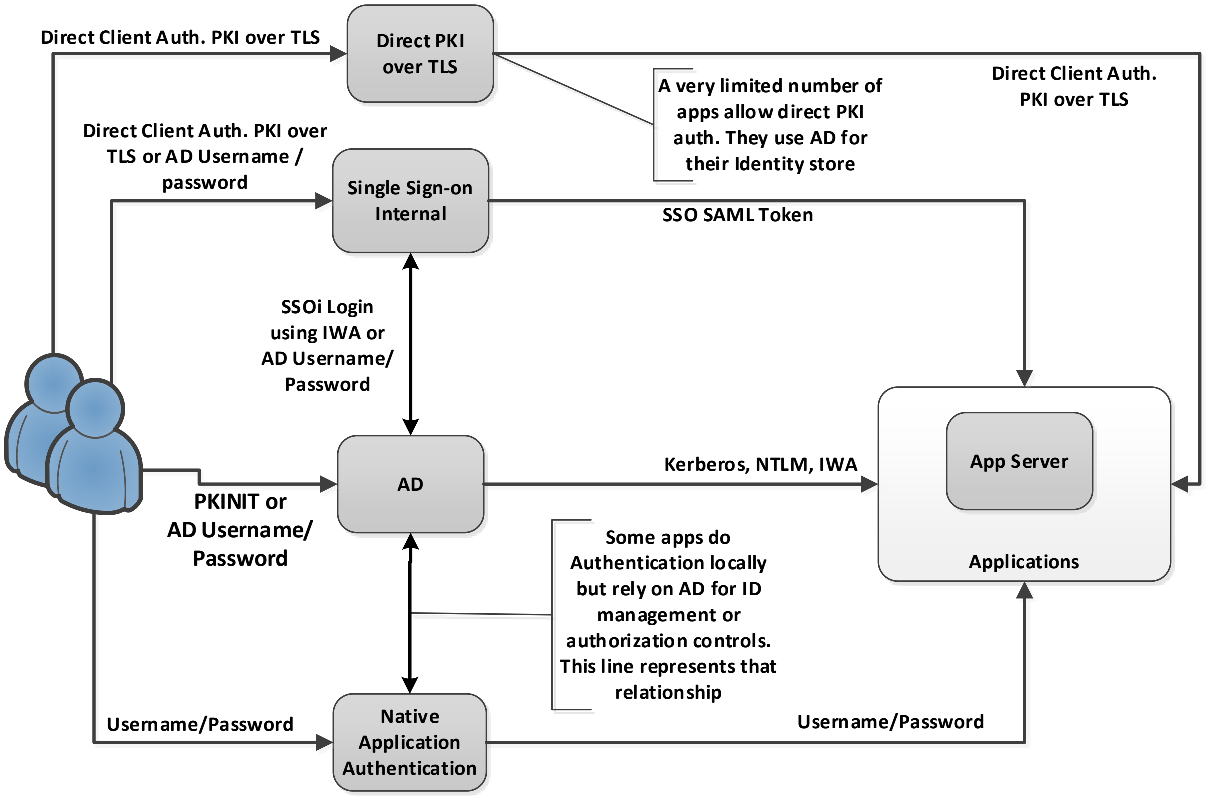
Direct Client Auth. PKI over TLS
Direct PKI over TLS
A very limited number of apps allow direct PKI auth. They use AD for their Identity store
Direct Client Auth. PKI over TLS
Direct Client Auth. PKI over TLS or AD Username / password
Single Sign-on Internal
SSO SAML Token
SSOi Login using IWA or AD Username/ Password
AD
Kerberos, NTLM, IWA
App Server
Applications
PKINIT or AD Username/ Password
Some apps do Authentication locally but rely on AD for ID management or authorization controls. This line represents that relationship
Username/Password
Native Application Authentication
Username/Password

Figure 2 – Current Internal User Identity Authentication

The primary VA user identity authentication protocols, as shown in Figure 2, include:

- **Application Specific Authentication** – Some applications natively authenticate users, maintaining their own user store (e.g., user authentication to VistA is currently natively supported using access and verify codes.)
- **Kerberos** – Many VA applications currently leverage a Microsoft (MS)-based token system to allow user authentication.
- **NTLMV2 –** This legacy MS protocol uses a three way handshake using password hashes where the client contacts the server which contacts the domain controller.
- **PKI Authentication** – VA network authentication and a limited number of applications use PKI technology. Currently the Enterprise Technical Architecture (ETA) Compliance Criteria requires all new applications to be PIV-enabled, and OMB 15-13 requires all web servers to use PKI technology to support HTTPS.
- **IAM SSOi** - Some applications have migrated to SSOi authentication services. SSOi can support PKI, AD username/password, or Integrated Windows Authentication (Kerberos) to authenticate a user and establish a SSO session. SSOi is only used by internal VA users.
- **IAM SSOe** – SSOe is used to authenticate external users to VA systems.

2.2 EXTERNAL AUTHENTICATION CAPABILITIES AND LIMITATIONS

IAM has implemented SSOe as an ESS to centralize external authentication. The diagram below depicts the current state of federated authentication services.

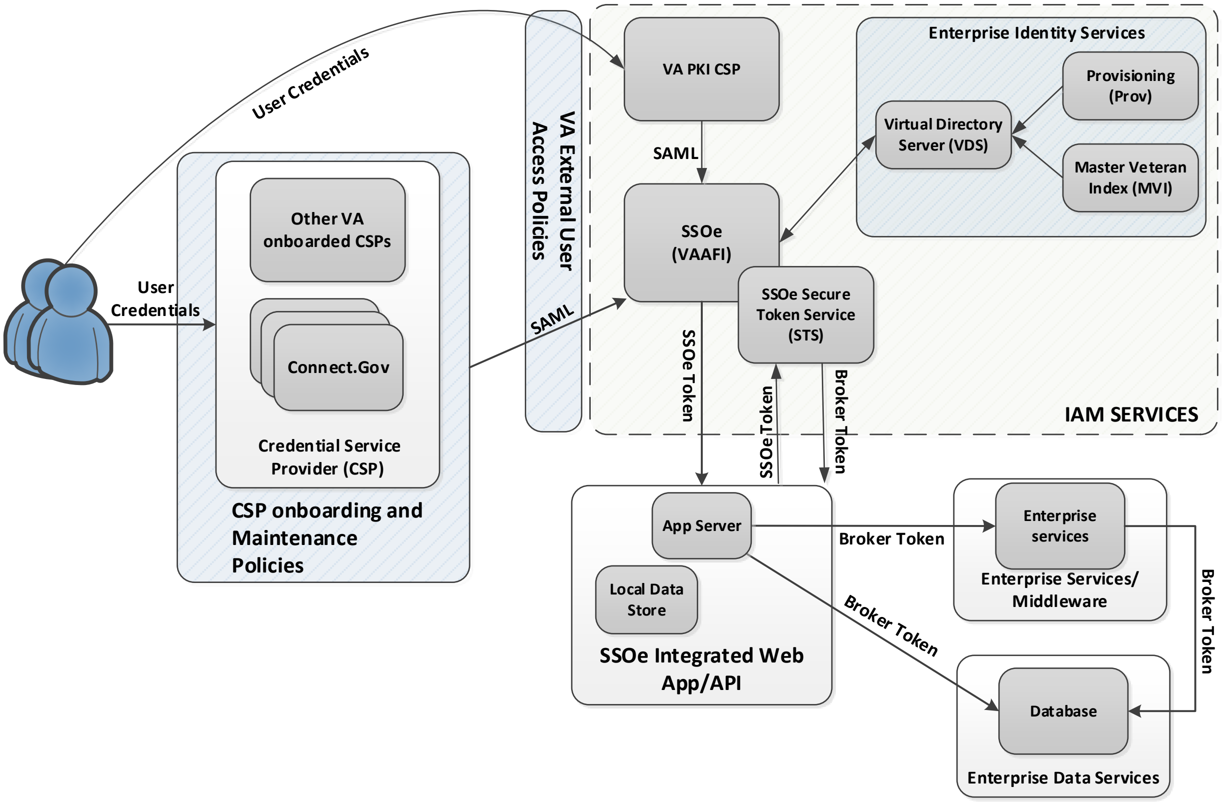
User Credentials
User Credentials
Other VA onboarded CSPs
Connect.Gov
Credential Service Provider (CSP)
CSP onboarding and Maintenance Policies
SAML
VA External User Access Policies
VA PKI CSP
SAML
SSOe (VAAFI)
SSOe Secure Token Service (STS)
Enterprise Identity Services
Provisioning (Prov)
Virtual Directory Server (VDS)
Master Veteran Index (MVI)
IAM SERVICES
SSOe Token
SSOe Token
Broker Token
App Server
Local Data Store
SSOe Integrated Web App/API
Broker Token
Broker Token
Enterprise services
Enterprise Services/ Middleware
Broker Token
Database
Enterprise Data Services

Figure 3 – Current External User Identity Authentication

Many Veteran-facing applications have not migrated to SSOe and continue to perform authentication within the application which creates compliance, audit and monitoring gaps. VA is currently leveraging SAML assertions based on traditional web services using Simple Object Access Protocol (SOAP) and XML. IAM uses SAML as the means to authenticate users from the external Identity Providers (IdP)/ CSP to SSOe. SAML and Federal Public Key Infrastructure (FPKI) are the only two currently approved Federal Identity, Credential, and Access Management (FICAM) Profiles[1]. It should be noted that OpenID 2.0 has been deprecated and is not approved for use. As only FICAM-approved providers are allowed, SAML use is projected for continued use. IAM can support OAuth using JavaScript Object Notation (JSON), but the current SAML attributes primarily support XML payloads with SOAP packaging. Additionally, while VA has implemented instances of OAuth for delegated application access, it currently does not have centralized governance of OAuth authorization servers. Limited governance of the OAuth instances poses security risks to interoperable data sharing and federated identity propagation.

[1] https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000Sfwe

3 FUTURE CAPABILITIES

User authentication for VA IT resources will be conducted in a manner that:

- Provides confidentiality by preventing unauthorized access.
- Provides integrity that protects against unintentional or malicious change.
- Provides availability of data for users.
- Integrates with Enterprise Shared Services to support proper auditing and monitoring.

All VA projects shall coordinate with IAM to determine appropriate integration requirements for IAM services, including the specific type(s) of identity credentials based on the sensitivity of the information that can be accessed, the strength of the identity credential, and the environment where the identity credential is being presented. The following sections describe the core foundations of the IAM SSO service and the guidance for SSOi and SSOe services.

3.1 CORE VA LOA CONCEPTS

All VA IT projects shall apply appropriate controls to the authentication protocol selected to ensure it meets the determined LOA requirements. Identity authentication for information systems and networks within VA must be conducted in a manner that:

1. **VA Applications shall be assessed and implement LOA requirements for authentication:** VA shall implement guidance in OMB 04-04 and NIST 800-63 to rate all existing applications to their appropriate LOA and enforce strict and appropriate security controls for user authentication to those applications. Detailed requirements for authentication at different LOAs are available in Appendix E.

2. **LOA for user authentication shall be determined by the weakest link in the authentication process:** All elements of the user's authentication to an application factor into the LOA rating of the authentication: the user's identity credential; the in-direct client authenticator; the secondary authentication token; and, the application. The lowest LOA for any of these credentials, systems, tokens, or applications shall be the LOA for the entire process. For example, if a user authenticates with direct PKI over transport layer security (TLS) using a PIV card (LOA 4), then user then requests access to an application which authenticates the user to the application using Kerberos (LOA 2). The LOA for this entire process would be LOA 2. Had the user attempted to access an application rated at LOA 3, the application or in-direct client authenticator should prompt the user to re-authenticate at the higher LOA.

3. **Application authentication protocols shall comply with all existing guidance established in VA 6500:** The LOA requirements outlined in NIST 800-63 are not the only requirements governing user authentication. All federal information systems must meet the minimum security requirements defined in FIPS 200. These requirements direct organizations to select/apply appropriate security controls as described in NIST 800-53. From this standard, VA's baseline

security controls are contained and detailed in VA 6500 Handbook. The combination of FIPS 200, NIST 800-53, and VA 6500 sets the foundational level of security for all information and information systems within VA. All foundational requirements in these documents that pertain to user authentication are required to be applied to the applications, systems, and authentication protocols within the authentication framework established by this document.

3.2 LEVELS OF ASSURANCE (LOA) ASSESSMENT

The OMB 04-04 describes four levels of identity authentication assurance levels, with Level 1 being the lowest level of assurance and Level 4 being the highest level of assurance. Each assurance level describes the degree of confidence that the user that presented a credential (e.g., a password) is in fact that user. It should be noted that the four (4) LOAs are established for the use of civilian agencies and do not apply to systems that rate as National Security Systems or contain classified or highly sensitive information. Standards for those systems are set by the National Security Administration (NSA) and are not described in this document.

The level of assurance needed is based on the consequence of authentication errors and/or misuse of credentials. As the consequences of an authentication error increase, the level of assurance should increase. Informal or low value requests will require less stringent assurance. Higher value or legally significant requests (e.g., HIPAA, PII) will require more stringent assurance.

Table 1 – Level of Assurance (LOA) Overview

LOA	Description	Technical Requirements			Example of credentials meeting requirements
		Identity Proofing Requirements	**Token (Secret) Requirements**	**Authentication Protection Mechanisms Requirements**	
1	Little or no confidence exists in the asserted identity; usually self-asserted; essentially a persistent identifier	Requires no identity proofing	Allows any type of token including a simple PIN	Little effort to protect session from offline attacks or eavesdropper is required.	Internal – N/A External – User name and password issued by CSP with no proofing.
2	Confidence exists that the asserted identity is accurate; used frequently for self-service applications	Requires some identity proofing	Allows single-factor authentication. Passwords are the norm at this level.	Online guessing, replay and eavesdropping attacks are prevented using FIPS 140-2 approved cryptographic techniques.	Internal – SSOi with option for Integrated Windows Authentication (IWA) and AD username/password. External – User name and password issued

					by CSP with remote identity proofing.
3	High confidence in the asserted identity's accuracy; used to access restricted data	Requires stringent identity proofing	Multi-factor authentication, typically a password or biometric factor used in combination with a 1) software token, 2) hardware token, or 3) one-time password device token	Online guessing, replay, eavesdropper, impersonation and man-in-the-middle (MitM) attack are prevented. Cryptography must be validated at FIPS 140-2 Level 1 overall with Level 2 validation for physical security.	Internal – SSOi with PIV as only option. External - User name and password issued by CSP with remote identity proofing and OTP code.
4	Very high confidence in the asserted identity's accuracy; used to access highly restricted data.	Requires in-person registration	Multi-factor authentication with a hardware crypto token (Use of bearer SSO is not permitted)	Online guessing, replay, eavesdropper, impersonation, MitM, and session hijacking attacks are prevented. Cryptography in the hardware token must be validated at FIPS 140-2 level 2 overall, with level 3 validation for physical security	Internal – Direct PIV External – N/A

Determining the LOA for an Application or System

Identified risks for a particular application should be mapped to a minimum assurance level based on potential impact. Assignment of impact to these risks is based on the context and nature of the people or entities affected by an improper authentication. For example, if five categories of potential impact are for Level 1 and one category of potential impact is for Level 2, the application should require Level 2 assurance.

To determine the required LOA, application managers and developers will follow OMB guidance. OMB outlines a five-step process by which agencies should meet their authentication assurance requirements.

1. **Conduct a risk assessment of the application/system** – NIST SP 800-30 offers a general process of risk assessment and risk mitigation. VA’s Office of Information Security shall provide additional guidance for conducting assurance risk assessments inside VA.
2. **Map identified risks to the appropriate assurance level** – OMB M-04-04 provides guidance for this mapping.
3. **Select technology based on authentication technical guidance** – VA’s default authentication solution is the use of IAM single sign-on for all user identity authentications. Applications that meet exception criteria may be required to use direct client authentication using PKI over TLS or may use Kerberos, if approved.
4. **Validate the implemented system has met the required assurance level** – OIT will use NIST SP 800-53A to conduct an assessment to determine if the application has met the required LOA standards.

5. **Periodically reassess the information system to determine technology refresh requirements** – NIST 800-37 revision 1 provides guidelines for periodic reassessments. Agencies should also follow assessment guidelines established in NIST SP 800-53 and VA policy related to Continuous Monitoring.

Guidance on Mapping Identified Risks to the Appropriate Assurance Level

As step #2 above indicates, the result of the risk assessment should be the mapping of the results to a corresponding LOA. Currently, a methodology with examples does not exist to demonstrate how this mapping is accomplished. In order for this process to be applied consistently across the enterprise, the risk categories should be explained with examples of what types of ratings would result in each of the Levels of Assurance. The sample table below is from the Centers for Medicare & Medicaid Services (CMS) Risk Management Handbook for CMS Authentication Standards. The handbook documents six impact categories that use Low/Moderate/High ratings with descriptions of each. Tables provides examples for each LOA including types of information and minimum LOA ratings based on risk ratings. This type of methodology will help ensure that security is not compromised by the lowering of LOA ratings to increase the ease of integration.

Table 2 – Level of Assurance Example[2] [3]

Information Type	Explanation and Examples	E-authentication Level			
Investigation, intelligence-related, and security information (14 CFR PART 191.5(D))	Information related to investigations for law enforcement purposes; intelligence-related information that cannot be classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements.	**Level 4**			
	Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
	Inconvenience, distress or damage to standing or reputation	Low	Mod	<Mod>	High
	Financial loss or agency liability	Low	Mod	<Mod>	High
	Harm to agency programs or public interests	N/A	Low	<Mod>	High
	Unauthorized release of sensitive information	N/A	Low	Mod	<High>
	Personal safety	N/A	N/A	Low	Mod/High
	Civil or criminal violations	N/A	Low	Mod	<High>

3.3 ADAPTIVE AUTHENTICATION REQUIREMENTS

NIST 800-53 control IA-10: Adaptive Identification and Authentication allows organizations to employ these adaptive authentication controls requiring users to provide additional authentication information based on assessed risks. This applies to two areas: **Step-Up Authentication and Adaptive Authentication.**

- ***Step-Up Authentication - Authentication protocols must have functionality in place to allow a user to re-authenticate to an appropriate LOA in order to access requested resources to which they have appropriate access rights.*** This "step-up" functionality allows the issuance of a new authentication challenge at any point in a user session during which an increase LOA authentication is necessary. For example, if a user authenticated at LOA 2 attempts to access an application at LOA 4, they will be prompted to use their PIV card.
- ***Adaptive Authentication - VA Authentication protocols must be designed to allow the network to issue occasional re-authentication challenges to users per established policy.*** This functionality will allow VA to re-authenticate users at their current or higher LOA

[2] (CMS Enterprise Information Security Group, 2016), https://www.cms.gov/research-statistics-data-and-systems/cms-information-technology/informationsecurity/downloads/rmh_viii_3-1_authentication.pdf

[3] Also see http://www.usda.gov/egov/egov_redesign/intranet/eauth/Assurance_Levels_Examples_v1.3.doc

based on perceived or established risks associated with a user's session, behavior, or other established policy.

The following are core concepts for implementing this capability:

1. **Implement LOA step up functionality and policy:** VA authentication protocols and applications must be able to trigger an LOA step up functionality that will require users who have accessed the network at a lower LOA to re-authenticate at a higher LOA when they attempt to access resources that are rated higher than their initial authentication would allow.
2. **Authentication protocols must support future role based (RBAC) and attribute based (ABAC) access control:** All approved authentication protocols must be implemented in a way that will support the enterprise in instituting role based and/or attribute based access control policies at the enterprise level.
3. **Implementation of functionality and policy to allow re-authentication challenges:** VA shall implement functionality and policies that allow re-authentication challenges to be issued to users based upon the future need for risk based access control.
4. **Implement capability to control and log-out user sessions:** VA authentication services must be able to monitor user sessions and ensure or force user log-out (single log-out) across all applications as needed.

3.4 INTEGRATION WITH ENTERPRISE SHARED SERVICES

The ProPath process (PRI-7) "Complete Identity Access Management Requirements" requires all projects evaluate their need for the use of ESS managed by the IAM team upon initiation. The following are core concepts for successful ESS delivery:

1. **Enterprise Shared Services shall be used to support authentication, authorization, and auditing:** VA has implemented ESS through IAM's AcS program which provides an enterprise provisioning service and user store, role based (RBAC) and attributed based (ABAC) access controls, authentication, and audit services.
2. **Create a single service to access all enterprise identity and attribute management stores: T**he Master Veteran Index (MVI) is the authoritative identity service within VA. However, MVI does not contain all attributes used as part of the authentication and authorization process. IAM AcS provides a Virtual Directory Server (VDS) which contains internal and external users and is integrated with the Provisioning identity store, Active Directory, MVI and external CSPs, but additional sources are still in progress. IAM will create and update a service as needed to serve as the primary source for federation of user identities and attributes across all VA.
3. **Applications shall rely on VA's central identity and attribute stores to conduct user authentication:** This includes migration of legacy applications from application-based authentication to use of ESS.
4. **Authentication protocols shall support VA's Service Oriented Architecture (SOA) environment:** As VA moves to a SOA environment all authentication protocols will be

implemented in a way that can support standards set by the SOA Enterprise Design Pattern.

5. **Applications shall support authentication protocols that support the implementation of enterprise wide role based (RBAC) and attributed based (ABAC) access controls:** An Enterprise Design Pattern based on Authorization will provide further guidance on these areas.

3.5 USER CREDENTIALS

All VA information systems and networks shall be capable of distinguishing and limiting user identity authentication to users who have presented identity credentials which meet the required LOA for the resource which they are attempting to access. In situations where automated credential checking is not available, the information system or network shall perform credential revocation checking in accordance with applicable credential policy**.** The information system shall validate during logon that the authenticator is bound to the identity credential used in the identity authentication process. The following are core concepts related to User Credentials:

1. **User credentials shall be appropriate for use in the requested environment:** Information system or VA network shall ensure that any credential used for identity authentication is appropriate for the authenticating entity's environment and the sensitivity level of the information for which the information system facilitates access.
2. **Information system or VA network shall ensure that any credential used for identity authentication has been issued by an approved VA identity credential provider or an approved federal or industry partner identity credential provider.**
3. **Information system or VA network shall verify that any identity credential used for identity authentication has not been revoked:** Information systems or the VA network must check to ensure that the identity credential presented has not been revoked by the identity credential provider or otherwise declared invalid.
4. **Information system or VA network shall only permit authentication to users who present identity credentials at or above the required LOA for the requested resource**

Types of User Credentials

The primary identity credentials available to internal VA users for identity authentication are:

- **VA-issued PIV Cards:** PIV cards and PKI authentication are LOA 4 credentials and are acceptable for authentication to all four LOAs depending on the authentication protocol used by the application. ***The PIV card is the default authentication identity credential for all internal VA users.***
- **One-time Password Tokens (OTP):** In some cases, VA will issue OTP tokens as a form of 2FA. A username and password with an OTP token is acceptable for authentication up to LOA 3 applications, however current OTPs are integrated with IAM.

- **Active Directory Username and Password:** AD username and password are LOA 2 credentials and are only acceptable for temporary authentication to LOA 2 or lower rated applications.
- **Other Credentials:** VA may choose to implement other identity credentials for allowing temporary access to VA network and applications. Any identity credential must be compliant with the NIST 800-63 LOA framework and guidelines, FICAM, FIPS, and VA 6500 security controls.

3.6 IDENTITY PROPAGATION

Because applications frequently need to call on middleware and other enterprise services to fulfill their functions, both the SSOi and SSOe infrastructures contain a Secure Token Service (STS). The STS allows integrated applications to exchange SSOi/SSOe tokens for brokered tokens in order to assert the authenticated user's identities to enterprise middleware and enterprise data services. This assertion of the user's identity is important as service calls traverse system boundaries. These secure assertions allow consuming systems to have some level of confidence that the calling application is interacting with an approved user. Additionally, the passing of tokens between systems can allow for additional user attributes to be passed that can enable RBAC and ABAC for authorization decisions and enable audit functions.

3.7 VA INTERNAL USER AUTHENTICATION

The following are core concepts of internal user authentication:

1. **Information systems shall only conduct internal user identity authentication using approved authentication protocols:** Coordination with IAM is required to confirm compliance.
    a. **Institute IAM SSOi as the default authentication protocol:** SSOi shall become the default authentication protocol within VA to include privileged account management. Exception criteria will direct the use of direct PKI or Kerberos as required.
    b. **Where required, VA shall enable use of PIV cards for authentication at the application layer:** LOA 4 applications shall be required to fully leverage the PIV credential using direct PKI over TLS.
    c. **Use of application-specific authentication protocols is prohibited:** all VA applications shall rely on enterprise authentication services and enterprise identity management services for user authentication, even if 2FA is used. ***Legacy systems that rely on native authentication processes will be evaluated and migrated to use an appropriate enterprise authentication protocol and enterprise identity management services.***
2. **Federal security standards governing user authentication including NIST SP800-53 and VA Handbook 6500 shall be followed.**
3. **Sufficient security controls within active directory and Kerberos shall be implemented:** VA shall ensure that its implementation of active directory and Kerberos within the

department meets best practices for information security and is able to support NIST 800-63 requirements for authentication (See following section on NTLM/Kerberos risks).

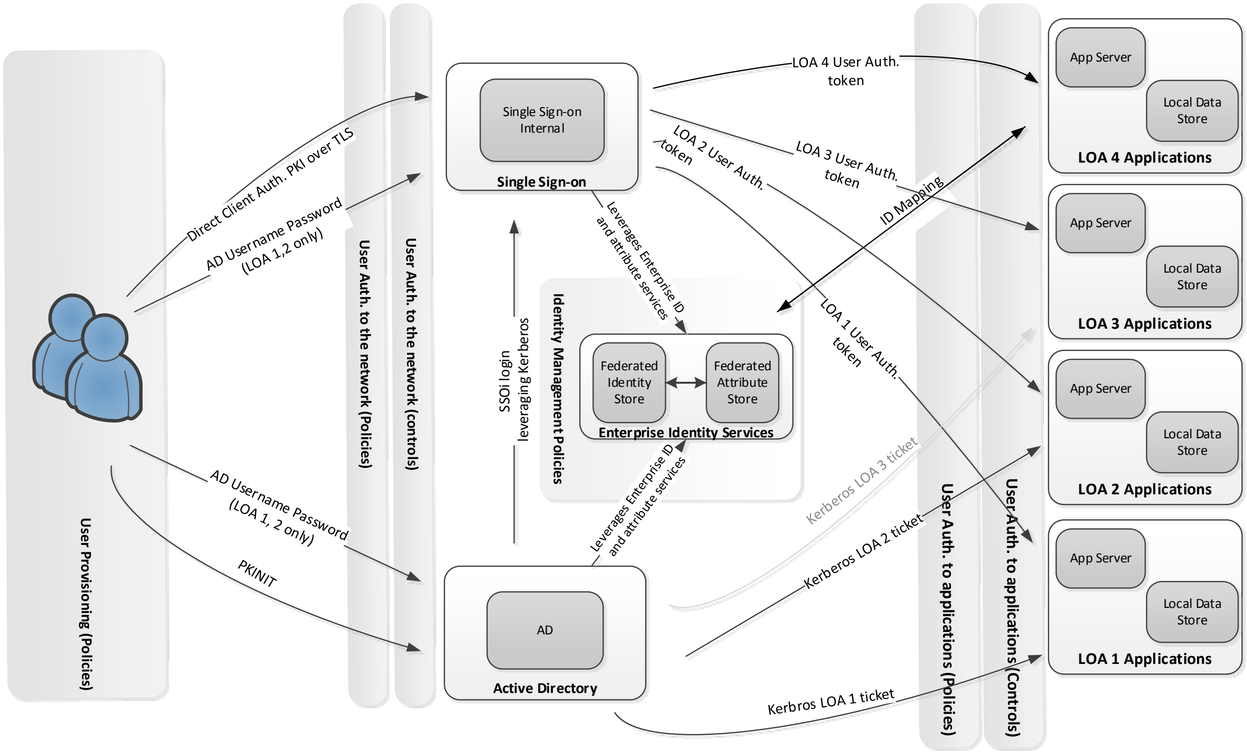

Figure 4 – Architecture Concept for Internal User Identity Authentication

The above architectural concept demonstrates the ability to authenticate to VA resources through the use of three primary identity credentials. A PIV card issued by VA will be the default identity credential and the only means of obtaining access to applications and networks rated at all four of the LOAs. OTP tokens will allow authentication up to LOA 3. The use of AD username and password will be maintained for use by users on a temporary basis, but will be restricted to authentication to applications rated at LOA 2 or lower. VA may choose to implement additional identity credentials to allow temporary access to applications and networks at a LOA equal to the identity credential selected.

The table below shows how VA authentication protocols for internal VA users map to the respective LOAs.

Table 3 – Authentication Protocol Mapped to LOA

	LOA 1	LOA 2	LOA 3	LOA 4

Direct PKI over TLS Direct PKI over TLS (PIV Card)	**X**	**X**	**X**	**X**
Single Sign-On Internal	**X**	**X**	**X**	(Not approved until holder of key technology is released and approved for use at LOA 4)
Kerberos (Active Directory Username and Password)	**X**	**X**	(Not approved under current AD and Kerberos implementation)	

SSOi is the default authentication protocol for all applications rated LOA 1-3. SSOi fully leverages the envisioned ESS for user authentication. Additionally the token technology used by SSOi is capable of fully supporting the envisioned SOA environment that VA is implementing under the VistA modernization program. Finally, SSOi can fully support the implementation of future enterprise RBAC, ABAC, and risk-based authorization controls that will further secure the VA environment.

SSOi Exception Criteria

During the feasibility assessment for integration with SSOi, it may become apparent that integration is not yet feasible. Some situations where exceptions to this criteria would apply are listed below:

- LOA 4 applications are required to use Direct PKI over TLS.
- LOA 3 or lower applications that, given special consideration by the application owner and the IAM team, feel that a higher LOA authentication protocol is needed, should implement Direct PKI over TLS.
- LOA 2 or lower rated application that is MS productivity software (e.g., MS Office or MS Email). Special consideration should be given to SharePoint. Some SharePoint sites may contain information that may require a more secure, LOA 3 or LOA 4, authentication protocol.
- LOA 2 or lower rated applications that natively support Kerberos and cannot support token based authentication (only applies to legacy applications).

- LOA 2 or lower rated MS application that is cost prohibitive to integrate with SSOi.
- Legacy application which uses Kerberos, does not meet any other exception criteria, and is being replaced with a SSOi or Direct PKI over TLS compliant system currently under design or development.
- Application has been reviewed by ASD and IAM and it has been determined it will not be integrated with SSOi

SSOi and LOA 4

In order for SSOi to be used to authenticate users at LOA 4, they must implement "holder-of-key-assertions". The Holder-of-Key assertion allows client public key and authorization information to be passed via a signed SAML token with integrity and confidentiality protection using mutual certificates. The current VA SSOi capability has not yet implemented holder of key assertions at LOA 4 and is therefore not approved for use at LOA 4 until it is demonstrated that the technology can sufficiently meet NIST 800-63 requirements at this LOA.

3.8 GUIDANCE RELATED TO THE USE OF ACTIVE DIRECTORY, KERBEROS AND NTLMV2

The use of assessments and authentication at the various LOAs is only effective if the integrity of the IAM architecture is secured. The following section addresses key areas related to the security of the authentication infrastructure itself.

Requirements for Current Active Directory Compliance

Due to the integral nature of AD within VA authentication systems, the implementation of the following requirements is considered a high priority.

- Kerberos tickets are not acceptable for use as assertions at LOA 4.
- Kerberos tickets are acceptable for use as assertions at LOA 3 only if:
  - All verifiers (Kerberos Authentication Servers and Ticket Granting Servers) are under the control of a single management authority that ensure the correct operation of the Kerberos protocol.
  - The subscriber authenticates to the verifier using a Level 3 or higher token (PIV card/OTP).
  - All LOA 3 requirements related to non-repudiation are satisfied.

Kerberos Exception Criteria:

Kerberos can continue to be used for:

- Legacy applications that cannot support token based authentication.
- Integrated MS products that do not require higher than LOA 2 (e.g., MS productivity software).
- Legacy applications that are currently being or will soon be replaced with SSOi or direct PKI over TLS compatible designs.

- Other applications that are determined on a case by case basis by the ASD and IAM BPMO teams.

NTLMv2 and “Pass the Hash” (PtH) Attacks

In order to protect plaintext passwords, Microsoft Windows NTLM and NTLMv2 hashes the password using an encryption algorithm and stores the hash. Authentication uses a challenge/response protocol where the authenticating server or domain controller issues a challenge which the client authenticates using the password hash as a key which the server compares to its own value to grant access. Any interactive user account authenticating to an endpoint, including domain admins, will create a hash when NTLMv2 is enabled. An attacker can steal these hashes and attempt to use them to gain access to other devices that are part of the domain which is known as “Pass the Hash” (PtH). By 2008, tools became widely available to dump passwords from LSASS in memory without needing to access the local storage. Advanced attackers will often target the domain controller where local admin permissions will give them access to the entire domain.

Kerberos and “Pass the Ticket”, “Silver Ticket” and “Golden Ticket” Attacks

In 2014, a newer version of the PtH attack surfaced (e.g., Mimikatz Toolkit) which targeted Kerberos tickets by stealing a Ticket Granting Ticket or Service Ticket from endpoints or delegated authorization servers[4]. Below is the typical Kerberos process:

1. User logs on with username and password, username+PIN, etc.
2. Password is hashed, a time stamp is encrypted with the hash and sent to the domain controller (DC).
3. The DC checks user information and grants a Ticket-Granting Ticket (TGT).
4. The TGT is encrypted, signed, and delivered to the user along with a session key.
5. The TGT is sent by the host to the DC when requesting service access i.e. a Ticket Granting Service (TGS) ticket. The DC opens the TGT and validates the PAC checksum. If the checksum is valid, data in the TGT is copied into the TGS. TGS is encrypted using the target service account hash and sent back to the host.
6. The host presents the TGS to the service which opens the ticket with its password hash.

The “Silver Ticket” forges a TGS meaning there is no communication with a DC. If an attacker can steal the hash of the KRBTGT account on a domain controller, they can forge the Kerberos Key Distribution Center (KDC) to create unlimited tickets, granting any level of access, with virtually unlimited lifetimes. This is the “Golden Ticket” attack. The reason for this is Microsoft’s MS-KILE specification (section 5.1.3): *“Kerberos V5 does not provide account revocation checking for TGS requests, which allows TGT renewals and service tickets to be issued as long as the TGT is valid even if the account has been revoked. KILE provides a check account policy (section 3.3.5.7.1) that limits the exposure to a shorter time. KILE KDCs in the account domain are required to check accounts when the TGT is older than 20 minutes. This limits the period that a client can get a ticket*

[4] Defending Against Pass-the-Ticket Attacks, http://www.identityweek.com/defending-against-pass-the-ticket-attacks/, August 5th 2015.

with a revoked account while limiting the performance cost for AD queries." The PAC (Privileged Attribute Certificate) is a structure contained in a Kerberos ticket that contains a list of privileges that the ticket is representing. PAC validation is disabled by default for accounts running as services which circumvents this time-based protection[5]. Attackers can also create new tickets to defeat this.

There are some significant risks to this attack since normally, many mitigation checks are performed before the ticket is created:[6]

- Systems trust the ticket validity. Therefore the ticket can state longer validity periods than set in domain policy, effectively bypassing policy.
- A user can continue to be impersonated even if the user password is changed.
- Bypasses SmartCard authentication requirements as it bypasses the usual checks the DC performs before creating the TGT.
- Can be used to persist on a domain and get access to all resources (Unless the KRBTGT account is changed).

Due to these risks, protecting Active Directory is a significant factor in some of these attacks. Microsoft has released patches and scripts, none of which resolve the issue. However, Microsoft has provided a way to change the password for the KRBTGT service account.

Effect of Using a SmartCard or PIV with NTLMv2 Enabled

When NTLMv2 is enabled for SSO, using a smartcard or PIV is similar to using a password. The hash of the SmartCard credentials are independent of the PIN. Windows creates a hash of the result to facilitate SSO so the user is not prompted repeatedly for their credentials. The end result is that the attacker could use the hash of the smartcard until its lifetime expires, which is considerably longer than the time for a password to expire in most cases.

What can be done to mitigate these attacks?

The following are mitigation strategies to be analyzed for implementation within the VA environment. These strategies and recommendations can help prevent both lateral movement and privilege escalation to decrease the impact of credential theft.

- **Protect the Authentication Infrastructure**
  Access to domain controllers should be restricted to authorized endpoints only. Application whitelisting should also be used to prevent the introduction of tools. Jump servers should be used to restrict access to the Authentication Infrastructure which also makes monitoring easier. A compromise that gains administrative access to a domain controller affects the integrity of the entire domain which is not resolved by resetting passwords unless the KRBTGT account is reset twice.

[5] http://passing-the-hash.blogspot.com/2014/09/pac-validation-20-minute-rule-and.html

[6] https://adsecurity.org/?p=1515

- **Reduce the Attack Surface**
  Establish separate AD forests in VA. Isolate devices in a forest where NTLMv2 is disabled from users and devices in the forest where NTLM is required.
- **Restrict lateral movement with HIPS Firewall Blocking**
  Compromise of some endpoints is to be expected. Using Host Intrusion Prevention System (HIPS) firewall filtering can help contain compromises on one endpoint from spreading to other endpoints (lateral movement) or domain controllers.
- **Remove standard users from the local administrators group**[7]
  This process is already underway and provides some protection against common malware, but it should be assumed advanced attackers will be able to escalate their permissions to local administrator regardless of the logged in user permissions.
- **Reduce Credential Availability to Attackers**
  Privileged domain accounts should not be used to login to workstations or other assets where domain management activity is not required.
- **Protect Privileged Accounts**
  In addition to using privileged domain accounts only where required, these accounts should be protected by 2FA. In compliance with OMB M 11-11, PIV should be used whenever possible.
- **Deny Local Accounts Network Logon**[8]
  The Local Administrator account often has the same password across the enterprise for convenience. Remove **network** and **remote interactive** logon privileges. This allows the password to remain consistent for support purposes while preventing use of this account for lateral movement across the domain.
- **Use Remote Management Tools that Do Not Place Reusable Credentials on the Remote Computer's Memory**
  Some remote authentication methods allow you to perform administrative tasks on the remote computer without storing the administrator account password hash, Kerberos ticket granting tickets (TGTs), or other reusable credentials on the remote computer's memory. Therefore, using only management tools with these authentication mechanisms can reduce the risk of PtH attacks as opposed to using domain admin or enabling Local Administrator accounts for remote use.
- **Audit All Authentication Events**
  The starting point for auditing to be effective is to identify what audit events signify a PtH, "Silver Ticket" or "Golden Ticket" attack is occurring. Auditing of application events in addition to Active Directory may be required to detect some attacks that do not communicate with the KDC. Microsoft's GoldenTicketCheck script starts by looking for non-standard ticket lifetimes.
- **Establish Incident Response Procedures in Coordination with Security Operations**

[7] ***Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques Whitepaper***: http://www.microsoft.com/en-us/download/details.aspx?id=36036

[8] **National Security Agency/Central Security Service| Information Assurance Directorate: Reducing the Effectiveness of Pass-the-Hash presentation**: https://www.nsa.gov/ia/_files/app/Reducing_the_Effectiveness_of_Pass-the-Hash.pdf

In some cases, a password reset will not resolve the risk of further compromise. Identify and document incident response procedures to different types of IAM compromises in advance.

- **Evaluate New Technology**

  In Windows 10, Microsoft claims to reduce the risk of authentication compromise through stealing of tickets by storing tickets within a secure container running on top of Hyper-V technology to prevent extraction[9]. This claim requires validation of its efficacy.

Because a wide variety of applications still leverage NTLMv2 for user authentication the cost for completely eliminating it from use on the network is seen as prohibitive. However, no new applications built or acquired by VA should use NTLMv2 for user authentication. Legacy applications that rely on NTLMv2 have high potential for abuse and require a plan for migration to a new authentication protocol if the application rates above LOA2 and contains sensitive information.

3.9 VA EXTERNAL USER AUTHENTICATION

VA implemented a consolidated SSOe approach for external authentication that enables projects such as MyVA. The current architecture contains the necessary services to allow application designers to perform a single integration with IAM SSOe in most cases, avoiding the need to integrate with many different CSPs. This architecture also allows external users to authenticate once to VA and gain access to many different resources. In this architecture the IAM SSOe platform is integrated with a number of CSPs, which are either externally or internally managed. The CSPs provide identity assertions in the form of SAML tokens to the VA Authentication Federation Service Provider (SP) within the SSOe infrastructure. Once received by the Federation SP, the token is validated and the SP brokers the connection from the user to the application. In the brokered connection, user information is passed to SSOe integrated applications in HTTP headers, called SSOe Tokens. The following are core concepts of this design:

1. **Applications employing authentication for users external to VA shall integrate with the enterprise IAM SSOe.** Applications shall not require application specific credentials for login but shall leverage the IAM architecture.
2. **IAM SSOe shall ensure that any credential employed for user authentication has been validated by a trusted and FICAM approvedCSP.**
3. **The authentication between the SP and the CSP shall be designed to maintain the confidentiality and integrity of the process.** The authentication process must be designed to protect against Cross-Site Request Forgery (CSRF), Cross Site Scripting (XSS), replay attacks, improper URI redirects, session fixation and other common authentication vulnerabilities.

[9] https://blogs.windows.com/business/2014/10/22/windows-10-security-and-identity-protection-for-the-modern-world/

4. **The IAM program for SSOe shall approve additional CSPs as needed to facilitate access to VA resources:** The IAM Business Program Management Office (BPMO) has developed requirements that manage the onboarding and integration of CSPs with SSOe. All CSPs are required to be FICAM compliant or submit to review and approval by IAM.
5. **Approved CSPs shall verify that any identity credential employed for identity authentication is valid at the time of presentation:** Information systems must check that the user credential presented has not been revoked by the identity credential provider or otherwise declared invalid.
6. **Information systems shall only authorize users who present credentials, to approved CSPs, at or above the required LOA for the requested resource.** All VA information systems and networks shall be capable of distinguishing and limiting user identity authentication to users who have presented identity credentials which meet the required LOA for the resource which they are attempting to access.

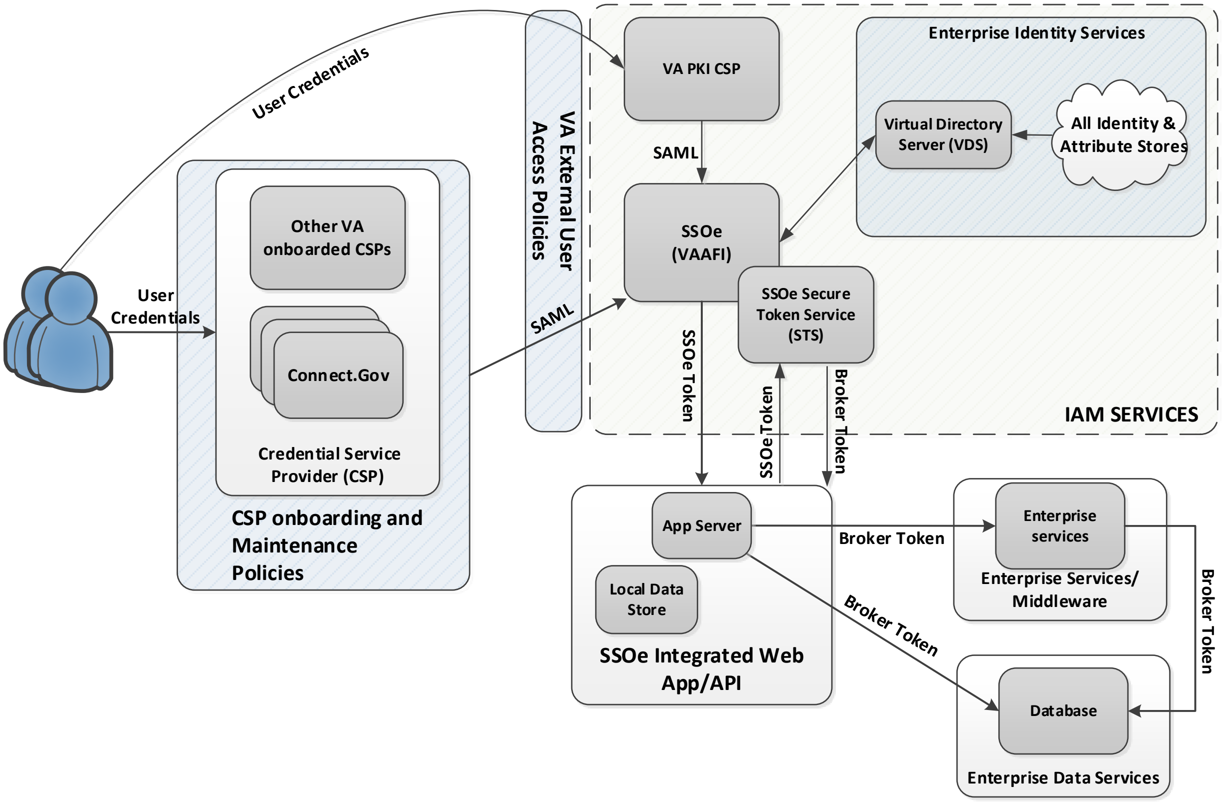
User Credentials
VA External User Access Policies
VA PKI CSP
Enterprise Identity Services
Virtual Directory Server (VDS)
All Identity & Attribute Stores
SAML
SSOe (VAAFI)
Other VA onboarded CSPs
User Credentials
Connect.Gov
Credential Service Provider (CSP)
CSP onboarding and Maintenance Policies
SAML
SSOe Secure Token Service (STS)
SSOe Token
SSOe Token
Broker Token
IAM SERVICES
App Server
Local Data Store
SSOe Integrated Web App/API
Broker Token
Enterprise services
Enterprise Services/ Middleware
Broker Token
Broker Token
Database
Enterprise Data Services

Figure 5 – Design Pattern for External User Identity Authentication

Application Integration with SSOe

As mentioned above, the design of the SSOe Infrastructure only requires application owners to integrate once with the SSOe to enable the full suite of authentication services that it provides. In order to facilitate integration with applications IAM has created a series of integration patterns for VA's Access Services. These include patterns for application owners to use to integrate with Single Sign-On External, Single Sign-On Internal, Credential Service Providers, Electronic Signature services, Identity Proofing, User Provisioning, Specialized Access Control, and Compliance Audit and Reporting (CAR) Services. Integration patterns are available by contacting IAM.

Support for Mobile Authentication

Mobile applications are most effective when designed to leverage the SSOe authentication framework. This framework will allow these applications to use FICAM compliant CSPs that have already been approved by VA. SSOe has solutions that support both native client and HTML. IAM solutions are designed to work in environments using SOAP-based architecture and can work with project teams to identify and provide solutions that work best for their user base. Furthermore, IAM can provide support for mobile authorization through the STS. More information on this topic is available in the Enterprise Design Pattern for Mobile Security.

VA CSP Approach

VA adopted a federated approach that allows the use of many different credential types to access VA resources. This approach allows external users to authenticate to requested VA information resources using the credential that is most convenient for them (given that it meets the proper LOA). The goal is to provide users with access to multiple VA resources without requiring separate authentication for each one. This approach achieves the goal of increasing access to VA resources while eliminating complexity for external users. VA has approved a number of external CSPs in order to support a variety of credentials and LOAs. VA will continue the process of approving CSPs as needed. The creation of Connect.Gov (formerly the Federal Cloud Credential Exchange [FCCX]) may reduce or eliminate the need for VA to separately approve CSPs on a case-by-case basis, and instead, would allow VA to leverage CSPs through Connect.Gov. Information concerning currently on-boarded CSPs can be obtained from the IAM office.

External CSPs and User Attributes

The IAM BPMO has established a formal process for evaluating and approving CSPs to provide user credentials to the enterprise. VA's future authentication and authorization environment will require that a 'rich' user profile (one that contains required user attributes) be provided to allow for proper implementation of access control services. IAM is working with Connect.Gov to ensure that all federally-approved CSPs implement and pass required attributes. This will allow the enterprise to securely authenticate and authorize users as needed. In addition, the ESS Security group has defined a common attribute set for the IAM SAML broker token. This standard is maintained and published by the ESS Security group in conjunction with the ESS governance bodies to provide application developers with an understanding of available user attributes.

Connect.Gov

Connect.gov is a cross-agency cloud service that would provide an "easy button" for federal agencies to use a wide range of FICAM-approved credentials, while allowing citizens to use private sector-issued credentials across multiple agencies and applications. By setting up a government-wide cloud service that handles the heavy lifting, each agency would only need to connect once to Connect.gov to take advantage of the increasing number of FICAM-approved third party credentials in the Identity Ecosystem. Connect.Gov adheres to the National Strategy for Trusted Identities in Cyberspace (NSTIC) Guiding Principles by developing a secure, privacy-enhancing, and easy-to-use solution for streamlining digital authentication. Further, Connect.gov will reduce costs for government agencies, improve the customer experience, and facilitate maturation of the Identity Ecosystem. Connect.gov is an initiative led by the White House being implemented with support from the U.S. Postal Service, the General Services Administration, and NIST's NSTIC National Program Office. If integrating an application with Connect.gov, the application LOA and required attributes must be provided. Connect.gov supports a limited set of attributes from Identity Services to Relying Parties by default[10].

3.10 ALIGNMENT TO THE TECHNICAL REFERENCE MODEL (TRM)

IAM SSOi/SSOe solution leverages approved tools and standards catalogued in the Technical Reference Model (TRM). The following table includes a mapping of technology categories to approved technologies and standards, and mandated ESS required by all VA projects.

Table 4 – List of Approved Tools and Standards for Enterprise Authorization

Technology Category	Example Technologies	Example Standards	Mandated ESS
• **Authentication**	SiteMinder, Active Directory	• X.509, OAuth/OpenID Connect, Kerberos, SAML, LDAP	• IAM Access Services
• **Authorization**	Axiomatics, DataPower	• XACML, LDAP	• IAM Access Services
• **Messaging**	WebSphere SOA Suite	• SOAP (legacy interfaces only), HTTPS (REST), JMS	• eMI
• **Encryption**	FIPS 140-2 compliant	• WS-*, TLS per FIPS 140-2 requirements	IAM Access Services
• **Cryptographic modules**	Cryptographic modules	• HTTPS	eMI API Gateway
• **Security Gateway**	SecureSpan, DataPower	• NIST SP 800-53, VA Handbook 6500	TBD

4 USE CASES

The following sections describe pertinent, real-world examples that apply enterprise authentication services such as SSOi and SSOe.

[10] http://www.connect.gov/agency-integration/

4.1 INTERNAL AUTHENTICATION TO OGC DATABASE

The Office of General Counsel is upgrading to a new solution to handle all casework related to internal investigations. The Program Manager has contacted IAM to determine the best method to provide secure authentication to the architecture designed.

- IAM reviews the system FISMA rating and risk factors and determines it requires authentication at LOA 4.
- IAM recommends Direct Client Authentication via PKI over TLS and provides supporting technical documentation.
- The user login is designed with the following process flow:
    - Internal VA user attempts to access the OGC application and the Logical Access Control System (LACS) prompts the user for authentication.
    - The User inserts PIV card into a card reader and inputs PIN.
    - PIV Application verifies response signature from PIV card authentication private key.
    - PIV Application performs Path Discovery and Validation (PD-VAL).
    - LACS validates the PIV credential using a PIV Authentication Key available on the card in accordance with appropriate, standards-compliant, path validation/ authentication techniques.
    - LACS checks Authority Information Access (AIA) for Online Certificate Status Protocol (OCSP) server information.
    - LACS contacts OCSP for revocation status or Certificate Revocation List (CRL) Distribution Points (CDP) to determine status and approves or revokes the request.
    - If successful, the LACS sends an assertion that includes any required attributes to the Application that the User is trying to access.

4.2 INTERNAL AUTHENTICATION TO A TEAM COLLABORATION SITE

A new project has started to assess and develop the use of an open source software into existing services. The team has requested a special source code repository for use with their Working Group, which includes members across multiple domains. The project sponsor wants the team to be able to collaborate efficiently without constantly having to authenticate to the site.

- IAM reviews the system FISMA rating and risk factors and determines it requires authentication at LOA 2 and is a candidate for SSOi.
- IAM provides technical documentation and guides the system owner through the integration process.
- The user login is designed with the following process flow:
    - User requests access to a web application integrated with the IAM ESS.
    - The web application redirects the request to the SSOi service.
    - User has already logged into their laptop and SSOi is able to use those credentials to authenticate.

    - The authentication data is passed back to the web application along with authorization data.
    - The web application determines permissions and grants access.

4.3 EXTERNAL AUTHENTICATION TO VA BENEFITS

In order to better serve Veterans as part of MyVA, several of the VA benefits services have contacted IAM to integrate with SSOe.

- IAM has collaborated with VBA to integrate several benefits applications of varying LOAs with SSOe.
- A possible user login might follow a process flow similar to below:
    - User opens the VA website and clicks on the URL to request a “Commissary and Exchange privileges” letter.
    - The website hosting the letter is LOA 2. The user is redirected to Connect.gov and asked to choose a CSP. The user selects DS Logon and is redirected to that CSP page and prompted to authenticate.
    - The user authenticates with their DS Username and Password and is prompted to consent to release of the requested attributes. The response is passed from the CSP back to Connect.Gov which passes the response to SSOe which communicates with the VA application.
    - The user navigates next to check their Compensation Claim Status. This web application is LOA 3. The user is redirected to Connect.gov and asked to choose a CSP. The user selects their DoD Common Access Card (CAC) and is redirected to that CSP page and prompted to authenticate.
    - The user inserts their CAC and enters the PIN.
    - The DoD CSP authenticates the user who is prompted to consent to release of the requested attributes. The response is passed from the CSP back to Connect.Gov which passes the response to SSOe which communicates with the VA application.
    - The user navigates to refill their prescription.
    - This web application is also LOA 3. The application connects with SSOe to authenticate the user and is provided the token for the last LOA 3 authentication.
    - The user is granted access to the prescription application.

APPENDIX A. SCOPE

This Enterprise Design Pattern describes the "to-be" state for VA internal (PIV-enabled VA employees, contractors, and volunteers) and external (business partners, veterans and others who access VA resources from outside the VA network) user identity authentication. In addition to describing the "static" rules for authentication, this document describes "adaptive" authentication tools that will be implemented and the need for authentication protocols that can support role-, attribute-, and risk-based access controls.

- This document does not address further authentication processes that may occur after internal users are authenticated, nor does it address standards for passing user authentication data for the purposes of making authorization decisions.
- This document does not address some IAM services in detail such as CAR, VA CSP, eSig and IP.
- This document does not address standards for passing user authentication data for the purposes of making authorization decisions (Please see future Authorization Enterprise Design Pattern).
- This document does not address requirements for authenticating devices (Please see the Non-Person Entity Security Design Pattern).
- This document is not a technical implementation guide, but is intended to guide application design by setting appropriate boundaries for designers. Information on technical implementation of these authentication protocols can be obtained from the appropriate OIT teams.
- While technologies (Token, Kerberos, Direct Client PKI) will be specified in this design document, the document is vendor agnostic.

Document Development and Maintenance

This design pattern was developed collaboratively with stakeholders from the ESS Security Group and included participation from VA's Office of Information and Technology (OI&T), Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). In addition, the Technology Strategies team engaged industry, external government agencies, and academic experts to review, provide input, and comment on the proposed pattern.

This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Office of Technology Strategies' lead for this document, who will facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

APPENDIX B. DEFINITIONS

Access – Interaction with a computer system for instance VistA. Such interaction includes data retrieval, editing (create, update, delete) and may result from a variety of technical mechanisms including traditional user log on, consuming applications exercising middleware based connectivity, SOA service requests, et cetera.

Accurate, unambiguous user identity – Information that represents the actual human that is interacting with a computer system, including the initiation of that interaction.

Application proxy – Construct involving the use of a generic, non-human “user” entity to represent “machine-to-machine” interaction where appropriate for interactions that do not involve a specific end user.

Auditing – The inspection or examination of an activity based on available information. In the case of computer systems, this is based on review of the events generated by the system or application.

Consuming application – The application consuming services from a provider system. Generally used when discussing a front-end application supporting a user, but even service providers can themselves be a consumer of other services.

Delegated Access – When an owner authorizes another to serve as his or her representative for access to a particular resource.

Enterprise Service Bus (ESB) – An SOA infrastructure device which manages message traffic, routing and a variety of other functions for instance orchestration, mediation, etc. The primary ESB at VA is the Enterprise Messaging Infrastructure (eMI).

Enterprise Shared Service (ESS) – A SOA service that is visible across the enterprise and can be accessed by users across the enterprise, subject to appropriate security and privacy restrictions.

Identity attributes – Characteristics which describe the user (e.g. name, National Provider Identifier, organization, etc.). Establishment of reasonably reliable “unique identity” is generally based on a combination of multiple identity attributes. Specific user identifiers include employee number and email address; may vary from organization to organization but identifier types ought to remain constant for all transactions from a specific organization.

Machine-to-machine interaction – In some cases, application processes resulting from workflow (not human interaction) will result in interaction with provider systems to download data, initiate background processing, etc. These actions are not directly initiated by a specific human and the interaction would be attributed to an application, possibly via a service account.

OAuth 2.0 - An open standard for authorization which provides clients a method to delegate access to server resources on behalf of a resource owner without sharing user credentials. OAuth 2.0 is not backwards compatible with OAuth 1.0.

Provider system – A system (e.g. VistA) which provides service at the request of a consuming application.

Representational State Transfer (REST) - An architecture style for designing client-server communications which is stateless and provides a uniform interface to access named resources using interconnected resource representations.

SAML token – An XML-based open standard data format for exchanging authentication and authorization data between parties.

System for Cross-Domain Identity Management (SCIM) - The SCIM Protocol is an application-level, REST protocol for provisioning and managing identity data on the web as described by IETF RFC 7642.

Service Oriented Architecture – A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations

User – A person who interacts with a computer system application. In this context, a “user” is not limited to VA staff members and may include persons from external organizations, patients, beneficiaries, designees, etc.

SSO and User Provisioning – A services provided by Identity and Access Management (IAM) for authenticating users and providing user provisioning information to other systems.

User types – traditional types including VA staff, staff of non-VA agencies (e.g. DoD), staff of private sector organizations (e.g. Walgreens), nontraditional, non-staff types including patients, beneficiaries, designees, sponsors, caregivers, etc.

APPENDIX C. ACRONYMS

Acronym	Description
AD	Active Directory
ADFS	Active Directory Federated Services (SSO based on SAML/WS-*)
API	Application Program Interface
ASD	Architecture, Strategy and Design
CDW	Corporate Data Warehouse
CPRS	Computerized Patient Record System
CSP	Credential Service Provider
eMI	Enterprise Messaging Infrastructure
ESB	Enterprise Service Bus
ESS	Enterprise Shared Service
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act
HTTPS	Hypertext Transfer Protocol over TLS
IAM	Identity and Access Management
IETF	Internet Engineering Task Force
MHV	MyHealtheVet
IdP	Identity Provider
JMS	Java Messaging Service
KAAJE	Kernel Authentication and Authorization for Java 2 Enterprise Edition
LDAP	Lightweight Directory Access Protocol
LoA	Level of Assurance
M4A	Minimum 4 Attributes
MDWS	Medical Domain Web Services
NIST	National Institute of Standards and Technology
PCI	Formally known as Payment Card Industry Data Security Standard (PCI-DSS)
PKI	Public Key Infrastructure
PIV	Personal Identity Verification
REST	Representational State Transfer
RFC	Request for Comment
RPC	Remote Procedure Call
SAML	Security Assertion Markup Language
SCIM	System for Cross-Domain Identity Management
SDD	System Design Document
SPML	Service Provisioning Markup Language
SOA	Service-Oriented Architecture

Acronym	Description
SSOe/SSOi	Single Sign-On External/Internal
TLS	Transport Layer Security
TPM	Trusted Platform Module
TRM	Technical Reference Model
VHA	Veteran Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
XML	Extensible Markup Language

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This Enterprise Design Pattern is aligned to the following VA OI&T references and standards applicable to all new applications being developed in VA, and are aligned to the VA ETA:

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA 6500 Handbook	• Directive information security program. • Defining overall security framework for VA.
2	VA	VA 6300 Directive	• Directive records and information management. • Defines information management framework for VA access services.
3	NIST	SP 800-53-4	• Special Publication — recommended security controls for federal information systems and organizations. • Defines the required security controls for IT systems under the Federal Information Security Management Act.
4	NIST	SP 800-63-2	• Special Publication — electronic authentication guideline. • Defines levels of assurance in user identities presented to IT systems over open networks. • Defines the data and procedural requirements for VA access services.
5	NIST	FIPS-201-2	• Federal Information Processing Standards Publication — PIV of federal employees and contractors. • Provides identity proofing, credentialing and chain of trust requirements and processes. • Defines the method for secure administrative interaction and control.
6	NIST	FIPS-140-2	• Federal Information Processing Standards Publication — security requirements for cryptographic modules. • Defines the cryptographic standards and requirements.
7	NIST	SP 800-122	• Guide to protecting the confidentiality of personally identifiable information (PII). • Provides technical procedures for protecting PII in information systems. • Defines the information that can be used to distinguish or trace an individual's identity.
8	OMB	M-04-04	• Memorandum to the heads of all departments and agencies – e-authentication guidance for federal agencies. • Defines the e-authentication requirement.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
9	GSA	FICAM	• Federal Identity, Credentialing and Access Management roadmap and implementation guidance. • Provides the common segment architecture and implementation guidance for federal ICAM programs.
10	White House	NSTIC	• National Strategy for Trusted Identities in Cyberspace – Provides guidance for identity trust in cyberspace.
11	US Congress	FISMA	• FISMA of 2002, Public Law 107-347.
12	US Congress	E-Government Act of 2002	• Federal management and promotion of electronic government services. • Defines the requirements for electronic services.
13	US Congress	The Privacy Act of 1974	• § 552a. Records maintained on individuals. • Defines VA access services privacy assessment and control requirements.
14	National Archives and Records Administration (NARA)	Federal Records Act	• Establishes the framework for records management programs in federal agencies.
15	VA	VA D 0735	• Homeland Security Presidential Directive 12 (HSPD-12) Program. • Defines department-wide policy, roles, and responsibilities for the creation and maintenance of systems and processes to implement VA's HSPD-12 Program necessary to implement HSPD-12 program.
16	OMB	M-05-24	• Implementation of HSPD 12 – policy for a common identification.

APPENDIX E. AUTHENTICATION LEVELS OF ASSURANCE

General Requirements LOA 4-2

Registration

- Records of registration shall be maintained by either the Registration Authority (RA) or by the CSP.
- Either the RA or the CSP shall maintain a record of each individual whose identity has been verified and the steps taken to verify their identity.
- The CSP shall have the capability to provide ID proofing records to Relying Parties (RP).
- If the RA and the CSP are remotely located and communicate over a network, the registration transaction between RA and CSP shall occur over a mutually authentication protected session.
- This transaction may consist of time-stamped or sequenced messages signed by their sources and encrypted for their recipient; in both cases approved cryptography is required.
- The CSP shall be able to uniquely identify each subscriber and the associated tokens and credentials issued to that subscriber.
- The CSP shall be capable of conveying unique IDs and associated tokens to verifiers.
- At all levels, PII collected as part of the registration process shall be protected.
- The applicant must supply full legal name, address of record, date of birth, and may be subject to policies established by the RA or CSP, and also supply other PII.

Tokens

- Two factors for authentication are sufficient to achieve the highest LOA.
- Memorized secret tokens are only appropriate for LOA 2 and 1.
- Pre-registered knowledge tokens are only appropriate for LOA 2 and 1.
- Look-up secret tokens are only appropriate for LOA 2 and 1.
- Out of band tokens are only appropriate for LOA 2 and 1.
- Single-factor one-time password devices are only appropriate for LOA 2 and 1.
- Single-factor cryptographic devices are only appropriate for LOA 2 and 1.
- Multi-factor software cryptographic tokens are appropriate for LOA 3, 2, and 1.
- Multi-factor one time password hardware tokens are appropriate for all LOAs.
- Multi-factor hardware cryptographic tokens are appropriate for all LOAs.
- Combinations of tokens can be used to achieve higher LOAs (e.g. two Level 2 tokens can be used to achieve LOA 3); details provided in NIST 800-63.

LOA 4

General LOA 4 Requirements

- Level 4 requires strong cryptographic authentication of all parties, and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used.
- The token secret shall be protected from compromise through the malicious code threat.
- Long-term shared authentication secrets, if used, shall never be revealed to any party except the claimant and CSP; however session (temporary) shared secrets may be provided to verifiers or RPs by the CSP. Strong, approved cryptographic techniques shall be used for all operations including the transfer of session data.
- All sensitive data transfers shall be cryptographically authenticated using keys that are derived from the authentication process in such a way that MitM attacks are strongly resisted.
- Level 4 assurance may be satisfied by client authenticated TLS (implemented in all modern browsers), with claimants who have public key MF hardware cryptographic tokens. Other protocols with similar properties can also be used.
- At LOA 4, only verified names may be specified in credentials and assertions.
- The token (or combination of tokens) used shall have assurance level of 4 or higher.
- The binding between the identity proofing and the token(s), if proofing is done separately from token issuance, shall be established at level 4.
- The authentication protocols used shall have Level 4 assurance level or higher.
- The token and credential management process shall use a Level 4 assurance level or higher.
- Authentication assertions (if used) shall have a Level 4 assurance or higher.

Registration Requirements Specific to LOA 4

- At LOA 4 the name associated with the subscriber shall be verified.
- AT LOA 4 only in person registration is permitted.
- For physical registration:
- The applicant shall identify himself in each new transaction through the use of a biometric that was recorded during a prior encounter.
- If the CSP issues permanent secrets, they must be loaded locally onto a physical device that is issued in person.

Token Requirements Specific to LOA 4

- Cryptographic module shall be FIPS 140-2 validated, Level 2 or higher, with physical security at FIPS 140-2 Level 3 or higher.
- For one time password hardware tokens:
- The one-time password shall be generated by using an approved block cipher or hash function to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password.
- The nonce may be a date and time, a counter generated on the device.
- Each authentication shall require entry of a password or other activation data through an integrated input mechanism.
- For hardware cryptographic tokens:
- shall require entry of a password, PIN, or biometric to active the authentication key.

- shall not allow export of authentication keys.

Token and Credential Management Requirements Specific to LOA 3

- No additional stipulations to LOA 3 credential storage requirements.
- No additional stipulations to LOA 3 token and credential verification service requirements.
- Sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process.
- All temporary or short-term keys derived during the original authentication operation shall expire and re-authentication shall be required after not more than 24 hours from the initial authentication.
- CSP shall have a procedure to revoke credentials within 24 hours.
- Verifiers or RPs shall ensure that the credentials they rely upon are either freshly issued (within 24 hours) or are still valid.
- All stipulations from LOA 2 and LOA 3 apply to records retention at LOA 4.
- The minimum record retention period for LOA 4 credential data is 10 years and six months beyond the expiration of revocation of the credential.
- The CSP must employ appropriately tailored security controls from the moderate baseline of security controls defined in NIST 800-53 and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.

Authentication Process requirements Specific to LOA 4

- LOA 4 must maintain threat resistance against: online guessing, replay, session hijacking, eavesdropping, phishing/pharming (verifier impersonation), MitM-strong, and denial of service/flooding.
- LOA 4 requires strong cryptographic authentication of all parties, and all sensitive data transfers between the parties.
- Either public key or symmetric key technology may be used.
- The token secret shall be protected from compromise through the malicious code threat.
- Long-term shared authentication code secrets, if used, shall never be revealed to any party except the claimant and the CSP.
- Session (temporary) shared secrets may be provided to the verifiers or RPs by the CSP.
- Strong, approved cryptographic techniques shall be used for all operations including the transfer of session data.
- All session data transfers shall be cryptographically authenticated using keys that are derived from the authentication process in a way that strongly resists MitM attacks.
- LOA 4 may be satisfied by client authenticated TLS with claimants who have public key MF hardware cryptographic tokens. Other protocols with similar properties can also be used.
- For multi-token schemes, the token used to provide strong resistance to MitM attacks is not required to be a hardware token.

Assertion Requirements Specific to LOA 4

- Bearer assertions (including cookies) shall not be used to establish the identity of the claimant to the RP.
- Assertions made by the verifier may be used to bind keys or other attributes to an identity.
- Holder-of-key assertions may be used, if:
  - the claimant authenticates to the verifier using a LOA 4 token in a LOA 4 authentication protocol;
  - the verifier generates a holder-of-key assertion that references a key that is part of the LOA 4 chain of trust; and,
  - the RP verifies that the subscriber possess the key that is references in the holder-of-key assertion using a LOA 4 protocol.
- The RP shall maintain records of the assertions it receives, allowing the RP to detect any attempt by the verifier to impersonate the subscriber using fraudulent assertions.
- Kerberos tickets are acceptable for use as assertions at LOA 4, if:
  - all verifiers (Kerberos authentication servers and ticket granting servers) are under the control of a single management authority that ensure the correct operation of the Kerberos protocol;
  - the subscriber authenticates to the verifier using a Level 4 token;
  - all LOA 4 requirements related to non-repudiation are satisfied.
- All LOA 1-3 requirements regarding protection of assertion data remain in force at LOA 4.

LOA 3

General LOA 3 Requirements

- LOA 3 provides multi-factor remote network authentication. At least two authentication factors are required. At this level, proofing procedures require verification of identifying materials and information. LOA 3 authentication is based on proof of possession of the allowed types of tokens through a cryptographic protocol.
- Multi-factor software cryptographic tokens are allowed at LOA 3.
- LOA 3 permits any of the token methods of LOA 4.
- LOA 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token against compromise by threats specified for LOA in NIST 800-63.
- At LOA 3, only verified names may be specified in credentials and assertions.
- The registration and identity proofing process shall, at a minimum, use Level 3 processes.
- The token (or combination of tokens) used shall have an assurance Level of 3 or higher.
- The binding between the identity proofing and the token(s), if proofing is done separately from token issuance, shall be established at Level 3.
- The authentication protocols used shall have a Level 3 assurance level or higher.
- The token and credential management process shall use a Level 3 assurance level or higher.
- Authentication assertions (if used) shall have a Level 3 assurance or higher.

Registration Requirements Specific to LOA 3

- The names associated with the subscriber shall be verified.
- Both in person and remote registration is permitted.
- Confirmation of a financial or utility account number is required.
- For remote registration:
  - The applicant shall identify himself in each new electronic transaction by presenting a temporary secret established during a prior transaction or encounter, or sent to the applicant's phone number, email, or physical address of record.
- For physical registration:
  - The applicant shall identify himself either by using the temporary secret described above or through use of a previously recorded biometric. Temporary secrets shall not be reused.
  - If the CSP issues permanent secrets, the must be loaded locally onto a physical device that is issued in person.

Token Requirements Specific to LOA 3

- Shall accept LOA 4 tokens.
- For multi-factor software cryptographic tokens:
  - The cryptographic module shall be validated at FIPS 140-2 Level 1 or higher.
  - Each authentication shall require the entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication.

Token and Credential Management Requirements Specific to LOA 3

- Files of long-term shared secrets used by CSPs or Verifiers at LOA 3 shall be protected by access controls that limit access to administrators and only those applications that require access.
- Shared secret files shall be encrypted so that:
  - the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation.
  - shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and is not exported in plaintext from the module.
- CSPs shall provide a secure mechanism to allow verifiers or RPs to ensure that the credentials are valid.
  - Mechanisms may include on-line validation servers or the involvement of CSP servers that have access to status records in authentication transactions
- Temporary session authentication keys may be generated from long-term shared secret keys by CSPs and distributed to third party verifiers as part of the verification services offered by the CSP, but long-term secrets shall not be shared with any third parties, including third party verifiers.

- Token and credential verification services categorized as FIPS 199 “moderate” or “high” for availability shall be protected in accordance with the contingency planning controls specified in NIST SP 800-53.
- Renewal and re-issuance shall only occur prior to expiration of the current credential.
- Claimants shall authentication to the CSP using the existing token and credential in order to renew or re-issue the credential. All interactions to do so shall occur over a protected session such as SSL/TLS.
- CSPs shall have a procedure to revoke credentials and tokens within 24 hours.
- Verifiers shall ensure that the tokens they rely upon are either freshly issued (within 24 hours) or still valid.
- All stipulations from LOA 2 regarding records retention apply.
- The CSP must employ appropriately tailored security controls from the moderate baseline of security controls defined in NIST 800-53 and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.

Authentication Process Requirements Specific to LOA 3

- LOA 3 must maintain threat resistance against: online guessing, replay, session hijacking, eavesdropping, phishing/pharming (verifier impersonation), MitM–weak, and denial of service/flooding.
- At LOA 3 at least two authentication factors are required.
- LOA permits any of the token methods of LOA 4.
- Strong cryptographic mechanisms shall be used to protect token secret(s) and authenticator(s).
- Long-term shared authentication secrets shall never be revealed to any party except the claimant and the CSP.
- Session (temporary) shared secrets may be provided to verifiers by the CSP, possibly via the claimant.
- Approved cryptographic techniques shall be used for all operations including the transfer of session data
- LOA 3 may be satisfied by client authentications TLS, with claimants who have public key certificates. Other protocols with similar properties may also be used.
- LOA 3 may also be met by tunneling the output of a MF OTP token, or the output of SF OTP Token in combination with a Level 2 personal password through a TLS session.

Assertion Requirements Specific to LOA 3

- Shall meet all LOA 2 requirements.
- Assertions shall be protected against repudiation by the verifier.
- All assertions shall be signed.
- Shall specify verified names and not pseudonyms.
- Kerberos tickets are acceptable for use as assertions at LOA 3.
    - Can only be used at LOA 3 if all verifiers (Kerberos authentication servers and ticket granting servers) are under the control of a single management authority that ensure the correct operation of the Kerberos protocol.
    - The subscriber authenticates to the verifier using a Level 3 token.

    - All LOA 3 requirements related to non-repudiation are satisfied.
- All single-domain assertions (web cookies) if used shall expire after 30 minutes if not used.
- Cross-domain assertions shall expire after five minutes if not used.
- Verifier may re-authenticate the subscriber prior to delivering assertions to the new RPs using a combination of long and short term assertions if:
    - the subscriber has successfully authentication to the verifier within the last 12 hours;
    - the subscriber can demonstrate that they were the party that authenticated to the verifier;
    - the verifier can determine if the subscriber has been in active communication with an RP since the last assertion was delivered by the Verifier, meaning that the subscriber has been actively using the services of the RP and has not been idle for more than 30 minutes.

LOA 2

General Requirements

- Shall permit any of the token methods of LOAs 3 and 4.
- Identification requirements requiring presentation of identifying materials or information are required for registration.
- Single factor authentication is allowed, including:
- memorized secret tokens, pre-registered knowledge tokens, look-up secret tokens, out of band tokens, and single factor one-time password devices.
- LOA 2 authentication requires that the claimant prove through a secure authentication protocol that he control an approved token.
- At LOA 2, online guessing, replay, session hijacking, and eavesdropping attacks shall be resisted, protocols are also required to at least weakly resist MitM attacks.
- At LOA 2, long-term shared authentication secrets, if used, are never revealed to any party, except verifiers operated by the CSP.
- Session (temporary) secrets may be provided to independent verifiers by the CSP.
- At LOA 2 all LOA 1 assertion requirements shall be met, in addition LOA 2 assertions shall be resistant to disclosure, redirection, capture and substitution attacks.
- Approved cryptographic techniques are required for all LOA 2 assertion protocols.
- The registration and identity proofing process shall, at a minimum, use Level 2 Processes or higher.
- The token (or combination of tokens) used shall have assurance Level of 2 or higher.
- The binding between the identity proofing and the token(s), if proofing is done separately from token issuance, shall be established at Level 2.
- The authentication protocols used shall have Level 2 assurance level or higher.
- The token and credential management process shall use a Level 2 assurance level or higher.
- Authentication assertions (if used) shall have a Level 2 assurance or higher.

Registration Requirements specific to LOA 2

- Records of registration shall be maintained by either the RA or by the CSP.

- Either the RA or the CSP shall maintain a record of each individual whose identity has been verified and the steps taken to verify his identity.
- The CSP shall have the capability to provide ID proofing records to RPs.
- If the RA and the CSP are remotely located and communicate over a network, the registration transaction between RA and CSP shall occur over a mutually authentication protected session.
- This transaction may consist of time-stamped or sequenced messages signed by their sources and encrypted for their recipient. In both cases, approved cryptography is required.
- The CSP shall be able to uniquely identify each subscriber and the associated tokens and credentials issued to that subscriber.
- The CSP shall be capable of conveying unique IDs and associated tokens to verifiers.
- At all levels, PII collected as part of the registration process shall be protected.
- The applicant must supply full legal name, address of record, date of birth, and may subject to policies established by the RA or CSP, and also supply other PII.
- At LOA 2, the identifier associated with the subscriber may be pseudonymous, but the RA and CSP shall retain the actual identity of the subscriber.
- Pseudonymous LOA 2 credentials shall be distinguishable from LOA 2 credentials that contain verified names.
- For electronic transactions:
    - The applicant shall identify himself in any new transaction beyond the first transaction or encounter by presenting a temporary secret which was established during a prior transaction or encounter or sent to the applicant's phone number, email address, or physical address of record.
- For in person transactions:
    - The applicant shall identify himself in person by either using a secret obtained in the same way as for electronic transactions or by biometric verification.

Token Requirements Specific to LOA 2

- For memorized secret tokens:
    - Memorized secret shall be a randomly generated PIN consisting of 6 or more digits, a user generated string consisting of 8 or more characters chosen from an alphabet of 90 or more characters, or a secret with equivalent entropy.
    - CSP shall implement dictionary or composition rules to constrain user-generated secrets.
    - Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts to 100 or fewer in 30 days.
- For look-up secret tokens:
    - Token authentication has 64 bits of entropy.
    - Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts to 100 or fewer in 30 days.
- For out of band tokens:

    - Token is uniquely addressable and support communication over a channel that is separate from the primary channel for e-authentication.
    - Verifier generated secret shall have at least 64 bits of entropy.
    - Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts to 100 or fewer in 30 days.
- For single-factor one-time password device:
    - Shall use approved block cipher or hash function to combine a symmetric key stored on device with a nonce to generate a one-time password.
    - Password shall have a limited lifetime, less than 30 minutes.
    - Cryptographic module performing the verifier function shall be validated at FIPS 140-2 Level 1 or higher.
- For single-factor cryptographic device:
    - Cryptographic module shall be validated at FIPS 140-2 Level 1 or higher.
    - Verifier generated token input has at least 64 bits of entropy.

Token and Credential Management Requirements Specific to LOA 2

- Files of shared secrets used by the CSP at LOA 2 shall be protected by access controls that limit access to administrators and only to those applications that require access.
- Files of shared secrets shall not contain plaintext passwords or secrets.
- Shared secrets must be protected:
    - Passwords may be concatenated to a variable salt and then hashed with an approved algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. Hashed passwords shall be stored in the password file. The variable salt may be composed using a global salt and the username or some other techniques to ensure the uniqueness of the salt within the group of passwords.
    - Or, shared secrets may be encrypted and stored using approved encryption algorithms and modes, and the needed secret decrypted only when immediately required for authentication.
    - Any method used to protect secrets at LOA 3 and 4 may be used at LOA 2.
- Long-term shared authentication secrets, if used, shall never be revealed to any other party except verifiers operated by the CSP.
- Session (temporary) shared secrets may be provided by the CSP to independent verifiers.
- Cryptographic protections are required for all messages between the CSP and verifier which contain private credentials or assert the validity of weakly bound or potentially revoked credentials.
- Private credentials shall only be sent through a protected session to an authenticated party.
- CSP shall establish suitable policies for renewal and re-issuance of tokens and credentials.

- Proof-of-possession of the unexpired current token shall be demonstrated by the claimant prior to the CSP allowing renewal and re-issuance.
- Passwords shall not be renewed; they shall be re-issued.
- After expiration of current token and any grace period, renewal and re-issuance shall not be allowed.
- Upon re-issuance, token secrets shall not be set to a default or reused in any manner.
- All interactions shall occur over a protected session such as SSL/TLS.
- CSPs shall revoke or destroy credentials and tokens within 72 hours after being notified that a credential is no longer valid or a token is compromised.
- If the issued credentials expire automatically after 72 hours then the CSP is not required to provide an explicit mechanism to revoke the credentials.
- CSPs that register passwords shall ensure that the revocation or de-registration of the password can be accomplished in no more than 72 hours.
- A record of the registration, history, and status or each token and credential (including revocation) shall be maintained by the CSP or its representative.
- Record retention period shall be seven years and six months beyond the expiration or revocation (whichever is later) of the credential.
- CSPs operated by or on behalf of an executive branch agency shall follow either the general records schedule established by the national archives or an agency-specific schedule as applicable.
- CSPs must employ appropriately tailored security controls from the low baseline of security controls defined in NIST 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.

Authentication Requirements Specific to LOA 2

- Shall permit the use of token methods used at LOAs 3 and 4.
- LOA 2 authentication requires the Claimant to prove through a secure authentication protocol that they control the token
- Session hijacking, replay, and online guessing attacks shall be resisted
- Shall be at least weakly Man-in-the-Middle resistant
- Session data transmitted between the Claimant and the RP following a LOA 2 authentication shall be protected as described in the NIST FISMA guidance
    - All session data exchanged between information systems that are categorized as FIPS 199 “moderate” or “high” for confidentiality and integrity, shall be protected in accordance with NIST 800-53 control SC-8

Assertion Requirements Specific to LOA 2

- If the subscriber name is a pseudonym, this information must be conveyed in the assertion.
- LOA 2 assertions shall be protected against manufacture/modification, capture, redirect and reuse.
- Assertion references shall be protected against manufacture, capture, and reuse.
- Each assertion shall be targeted for a single RP.
- RP shall validate that it is the intended recipient of the incoming assertion.
- All LOA 1 assertion requirements apply.

- Assertions, assertion references and any session cookies used by the verifier or RP for authentication purposes shall be transmitted to the subscriber through a protected session linked to the primary authentication process in such a way that session hijacking attacks are resisted.
- Assertions, assertion references and session cookies shall not be subsequently transmitted over an unprotected session or to an unauthenticated party while they remain valid.
- Any session cookies used for authentication purposes shall be flagged as secure.
- Redirects used to forward secondary authenticators from the subscriber to the RP shall specify a secure protocol such as HTTPS.
- Assertions sent from the Verifier to the RP, either directly or through the subscriber's device, shall either be sent via a mutually authenticated protected session between the verifier and RP or equivalently shall be signed by the verifier and encrypted for the RP.
- All assertion protocols used at LOA 2 require use of approved cryptographic techniques.
- Kerberos keys generated from user generated passwords are not approved above LOA 2.

LOA 1

General Requirements

- Shall permit any of the token methods of LOAs 2, 3, and 4.
- LOA 1 authentication requires that the claimant prove through a secure authentication protocol that he possesses and controls an approved token.
- Plaintext passwords or secrets shall not be transmitted across a network.
- Simple password challenge-response protocols are allowed.
- At LOA 1, long-term share authentication secrets may be revealed to verifiers.
- At LOA 1, assertions and assertion references shall be protected from manufacture/modification and reuse attacks.
- The registration and identity proofing process shall, at a minimum, use Level 1 processes or higher.
- The token (or combination of tokens) used shall have assurance level of 1 or higher
- The binding between the identity proofing and the token(s), if proofing is done separately from token issuance, shall be established at Level 1.
- The authentication protocols used shall have level 1 assurance level or higher.
- The token and credential management process shall use a Level 1 assurance or higher.
- Authentication assertions (if used) shall have a Level 1 assurance or higher.
- At LOA 1, the name associated with the subscriber is provided by the applicant and accepted without verification.

Registration Requirements Specific to LOA 1

- Shall recognize the use of pseudonymous credentials.

Token Requirements Specific to LOA 1

- For memorized secret tokens:

  - Shall contain 6 or more characters chosen from an alphabet of 90 or more characters, a randomly generated PIN consisting of 4 or more digits, or a secret with equivalent entropy.
  - Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts to 100 or fewer in 30 days.
- For Pre-Registered Knowledge Tokens:
  - Shall provide at least 14 bits of entropy.
  - The entropy in the secret cannot be directly calculated (e.g. user chosen or personal knowledge questions).
  - Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts to 100 or fewer in 30 days.
  - Verifier shall verify the answer provided for at least three questions.

Token and Credential Management Requirements Specific to LOA 1

- Files of shared secrets used by verifiers at LOA shall be protected by access controls that limit access to administrators and only to those applications that require access.
- Files that contain shared secrets shall not contain plaintext passwords.
- Any method used for long term protection of long-term shared secrets at LOA 2 and above may be used.
- Long term token secrets should not be shared with other parties unless absolutely necessary.

Authentication Requirements Specific to LOA 1

- Shall permit the use of any token methods of LOA 2, 3, and 4.
- LOA 1 authentication requires that the Claimant prove, through a secure authentication protocol, that he or she possess and controls the token.
- Plaintext passwords or secrets shall not be transmitted across the network.
- At LOA 1 long-term shared authentication secrets may be revealed to Verifiers.

Assertion Requirements Specific to LOA 1

- At LOA 1 it must be impractical for an attacker to manufacture an assertion or assertion reference that can be used to impersonate the subscriber.
- In a direct assertion model, the assertion which is used shall be signed by the verifier or integrity protected using a secret key shared by the verifier and RP.
- In an indirect assertion model, the assertion reference shall have a minimum of 64 bits of entropy.
- Bearer assertions shall be specific to a single transaction.
- If assertion references are used, they shall be freshly generated whenever a new assertion is created by the verifier (bearer assertions and assertion references are for one-time use).
- All assertions sent from the verifier to the RP shall either be signed by the verifier or transmitted from an authenticated verifier via a protected session.
- A strong mechanism must be in place to allow the RP to establish a binding between the assertion reference and its corresponding assertion based on integrity protected communications with the authenticated verifier.

- Assertions that are consumed by an RP which is not part of the same internet domain as the verifier shall expire if not used within five minutes.